News from Ed Markey

United States Congress **Massachusetts Seventh District**
FOR IMMEDIATE RELEASE **CONTACT: Tara McGuinness**
June 17, 2005 **(202) 225-2836**

REP. MARKEY: "MASTERCARD SECURITY BREACH: PRICELESS"

Personal Data and Credit Card Numbers of 40 Million Customers Compromised

Washington, DC: A Friday summer afternoon, 5:10 pm MasterCard International quietly announces a security breach that could affect over 40 million cards of all brands, of which nearly 14 million are MasterCard-branded.

According to press reports, the breach occurred at CardSystems Solutions in Tucson, which processes transactions on behalf of financial institutions and merchants.

In response to MasterCard's announcement earlier today, Representative Edward J. Markey (D-MA), a senior member of the House Energy and Commerce Committee, Co-Chair of the Congressional Privacy Caucus and author of three bills aimed at protecting consumer privacy and stopping identity theft, issued the following statement:

"Holding up a Liquor Store: $250.00."
"Robbing a Bank: $17,500.00."
"Car Jacking: $13,000."
"MasterCard Security Breach (40 million customers): Priceless."

"Today's announcement only underscores the need for new federal legislation to protect American consumers from the unending stream of revelations from corporate America about failure after failure to protect the public from data security breaches. I have introduced legislation that would protect consumers and provide more rigorous standards for companies who engage in the buying and selling of personal identifiers."

Rep. Markey introduced three bills in the 109th Congress to protect consumers from identity theft:

H.R. 1078: The Social Security Number Protection Act

This bill is aimed at protecting consumers from the abuse of the purchase and sale of social security numbers by:

- Making it crime for a person to sell or purchase Social Security numbers.
- Providing the FTC with rulemaking authority to restrict the sale of Social Security numbers, determine appropriate exemptions, and to enforce civil compliance with the bill's restrictions.

- Authorizing the states to enforce compliance, and provide for appropriate penalties.

H.R. 1080: The Information Protection and Security Act

This bill would give the Federal Trade Commission (FTC) power to oversee previously unfettered information brokers the same way it governs credit bureaus that handle private financial information. Currently, unregulated data brokers are able to sell files containing Social Security numbers, credit reports and other personal data by:

- Subjecting information brokers like ChoicePoint to federal regulation by the Federal Trade Commission, and specifically, requiring such brokers to comply with a set of new fair information practice rules that the FTC would be required to issue within 6 months of enactment.
- Mandating that the FTC rules require information brokers to better secure the information in their possession, grant consumers the right to obtain access to and correct information held by the broker, require information brokers to protect information from unauthorized users, and prohibit users of an information broker to obtain the information for impermissible or unlawful purposes.
- Creating regulations that are enforceable through the FTC, which would be empowered to bring civil actions to punish and fine violators;

H.R. 1653: The Safeguarding Americans from Exporting Identification Data (SAFE ID) Act

"The Safeguarding Americans from Exporting Identification Data (SAFE ID) Act," would prohibit companies from transferring personal information to any person outside the United States without notice and consent by:

- Requiring notice to a consumer from any business enterprise that wishes to transfer to a foreign country that consumer's personally identifiable information, such as the citizen's name, address, financial information, medical records;
- Requiring the Federal Trade Commission ("FTC") to determine whether the privacy protections of a country to which data is outsourced are, or are not, "adequate and enforceable;"
- Giving consumers the option to "opt out" of information transfers to countries with "adequate and enforceable" privacy protections, such as the European Union (EU);
- Barring companies from refusing to provide goods or services to consumers who elect to exercise their "opt out" or "opt in" consent rights, or from charging consumers more if they chose to exercise such rights;
- Providing for enforcement of the bill's restrictions by the FTC by defining violations of the bill as a violation of the Federal Trade Commission Act's prohibition on unfair and deceptive acts or practices, thereby allowing the FTC to seek injunctions against violators and to impose financial penalties of up to $11,000 per violation, for countries with "inadequate or unenforceable" privacy protections;
- Providing for additional civil remedies against violations, including authorization to the state attorney's general to bring civil actions to enjoin violations and impose monetary penalties of actual monetary losses or up to $10,000 per violation, whichever is greater; and
- Providing a citizen whose privacy rights are violated with a private right of action to sue a business who has violated the act for actual monetary damages or up to $10,000 per violation, whichever is greater.

For more information on Rep. Markey's legislation to protect consumer privacy check out: http://www.house.gov/markey/